ISSLP

Original Research

A Comparative Analysis of Iranian Criminal Policy and English Criminal Policy (in the Narrow Sense) Regarding Sexual Violence in Cyberspace

Alireza. Jahangiri[1], Soudabeh. Rezvani[2], Ruheddin. Kord Alivand[3]

[1] PhD Student, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran
[2] Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, Kharazmi University, Tehran, Iran
[3] PhD, Department of Criminal Law and Criminology, Lecturer, University of Poitiers, France

*** Corresponding author email address**: arz.jahangiri@gmail.com

Received: 2025-06-08 **Revised:** 2025-10-20 **Accepted:** 2025-10-27 **Published:** 2026-05-01

Cyberspace has for many years become an inseparable part of human life worldwide, permeating virtually all social, cultural, and economic relations. This development has brought about profound changes in the phenomenon of sexual violence and has generated new forms of violent conduct, while simultaneously transforming and expanding the populations of perpetrators and victims, as well as the environments and territorial dimensions in which such violence occurs. In light of these developments, the principal issue addressed in the present study is a comparative analysis of Iranian criminal policy and English criminal policy concerning sexual violence in cyberspace. To achieve this objective, the criminal policies of the two countries, Iran and England, were specifically compared on the basis of substantive laws governing criminalization and the determination of penalties. With respect to the research methodology, the documentary method was employed for the collection of the evidence and information required to explain and assess the research hypotheses and central research problem, while the descriptive-analytical method was used for evaluating and interpreting the collected data. The findings ultimately indicate that, in Iran, “sexual violence” has not yet been criminalized as a distinct and comprehensive category. Although cybercrimes have been criminalized under an independent statute, namely the Computer Crimes Act, no direct reference has been made to sexual violence committed in cyberspace. In England, although a distinct criminal policy framework has been established with respect to sexual violence committed in the physical environment, the legal provisions concerning such conduct in cyberspace have not yet been consolidated and remain dispersed across various legislative instruments. Accordingly, aligning Iran’s criminal policy concerning sexual violence with the laws and regulatory approaches of countries that have taken a more advanced position in this field constitutes an evident necessity.

Keywords: *criminal policy, sexual violence, cyberspace, criminalization, punishment*

How to cite this article:
Jahangiri, A., Rezvani, S., & Kord Alivand, R. (2026). A Comparative Analysis of Iranian Criminal Policy and English Criminal Policy (in the Narrow Sense) Regarding Sexual Violence in Cyberspace. *Interdisciplinary Studies in Society, Law, and Politics, 5*(3) 1-17. https://doi.org/10.61838/kman.isslp.282

1. Introduction

Cyberspace may perhaps be regarded as the most significant characteristic and distinguishing feature of the early decades of the twenty-first century compared with preceding centuries. The Internet, as a global communications network, has transcended national borders, offered a new conception of the social world of human beings, and transformed their lifestyles. It is evident that the Internet, as a product of the

© 2026 The authors. Published by KMAN Publication Inc. (KMANPUB). This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

technological revolution, together with the social networks that have emerged from it, encompasses both positive and negative dimensions and simultaneously carries intertwined opportunities and threats, much like other domains of the modern world. Accordingly, the Internet possesses a dual nature and inherent contradictions, and its utilization requires the management and regulation of diverse dynamics manifested through social networks and virtual communication channels. On the basis of this reasoning, it may be stated that one of the harms associated with cyberspace is the favorable environment it provides for cyber offenders because of the transnational nature of this network and the anonymity of its users.

Indeed, the criminogenic potential of cyberspace and the emergence of new and novel forms of crime constitute one of its adverse consequences, compelling governments either to adopt new criminal policies or to revise their existing criminal policies in accordance with cybercrime. In this context, violence in general, and sexual violence in particular, constitutes a category of crime which, although it has long existed in the offline environment and is not a novel criminal act, has undergone significant transformations and acquired complex dimensions in cyberspace, both formally, through the use of new instruments of violence, and substantively, because of the harmful and often concealed consequences it produces in the psychological and even physical lives of victims. Accordingly, legislative, judicial, and executive policymaking concerning sexual violence in cyberspace constitutes a challenge that, once conceptually formulated, may become one of the most acute problems of cyberspace in the future and therefore require extensive scholarly investigation. Hence, the present study seeks to examine sexual violence in cyberspace comparatively from the perspective of the criminal laws and criminal policies of Iran and England and, by taking substantive and procedural laws as criteria—including criminalization, punishment, crime detection, criminal procedure, and enforcement of sentences—to determine the position of cyber sexual violence within the legal systems of the two aforementioned countries.

2. The Impact of Cyberspace on the Phenomenon of Sexual Violence

Sexual violence is one of those forms of violence originating in the physical world that, in the age of widespread media and virtual networks, is also reproduced in cyberspace, although through forms, methods, and manifestations compatible with this emerging environment. Although sexual violence is not limited to women and girls, and adolescents and children are also among its victims, the reality is that women constitute the principal group victimized by sexual violence, and the phenomenon is associated with women more than with other social groups. In support of this proposition, reference may be made to a study entitled "Sexual and Gender-Based Harassment in Cyberspace," conducted in 2016 through online platforms such as Facebook, Twitter, Telegram channels, and Telegram groups. The questionnaire was shared with users from January 17 to February 1, 2016, and over a two-week period, 623 participants completed and submitted it. The findings revealed a very high prevalence of sexual violence in cyberspace. According to the results, 38% of respondents had directly experienced sexual or gender-based harassment online; 83.3% identified monitoring a person online and causing discomfort, 82.2% identified sending sexual or harassing messages and requests through messaging applications, 80% identified misuse of an individual's online information or photographs, and 76.6% identified contacting or threatening to contact a person's family in order to disclose private relationships as among the most prevalent forms of sexual violence and harassment in cyberspace (Hematpour, 2017).

Furthermore, Patricia Welch, a scholar in the field of cultural harms against women, argues in this regard that women, when confronting stereotypical attitudes in Internet environments, adopt certain strategies in order to engage in "interaction." Nevertheless, the Internet may provide more hostile environments, and in some of these environments women are particularly vulnerable and experience discomfort because men, in the terminology of Susan C. Herring, tend to adopt aggressive and dominance-seeking approaches. Consequently, some websites constitute environments of gratification and moral deterioration for young men and tempting environments for some women (Shadmani, 2015). Moreover, studies and reports concerning the impact of cyberspace on sexual and gender-based

violence indicate that online harassment, public shaming, planning physical harm, sexual assault, murder, and encouragement of suicide constitute some of the prevalent forms of sexual violence against women and girls in cyberspace (Hematpour, 2017).

In this regard, reference may also be made to the report of the United Nations Broadband Commission, according to which approximately one-third of women are exposed online to some form of cyber sexual violence. Several findings of this report may be summarized as follows: (1) approximately 73% of women have encountered or experienced some form of online violence; (2) women between the ages of 18 and 24 are the group most likely to encounter sexual harassment, sexual violence, and physical threats; (3) approximately nine million women across the 28 Member States of the European Union had experienced gender-based violence by the age of 15; (4) one-fifth of female Internet users live in countries in which online sexual harassment and violence against women are not subject to effective judicial enforcement; and (5) in many countries, women are reluctant to report cyber sexual violence committed against them because of fear of its social consequences (Fattahian, 2017). Likewise, a 2014 academic study conducted by the University of Maryland in the United States indicated that female users were, on average, 25 times more likely than male users to receive threatening messages, insults, messages containing obscene and sexist expressions, and verbal violence, and that victims of such violence were predominantly women aged 18 to 30. In many countries, moreover, women are reluctant to report cyber sexual violence committed against them because of fear of social consequences (Hematpour, 2017). Thus, sexual violence constitutes one of the most prominent forms of violence to have found a new arena for manifestation as a result of technological development and the globalization of communications. One such arena is cyberspace, an environment in which anonymity and the relative absence of effective regulation enable individuals to violate real-world norms with greater ease and pursue inhumane desires (Fattahian, 2017).

3. Manifestations of the Transformation of Sexual Violence in Cyberspace

The impact of cyberspace, however, has not been limited to increasing the incidence of sexual violence; rather, it has itself transformed sexual violence in dimensions such as new forms of conduct, new categories of victims, and new categories of perpetrators, which are examined below.

3.1. From the Perspective of New Forms of Conduct

Cyberspace is a relatively recent phenomenon, whereas violence is as old as human existence. It is therefore evident that, with the expansion of cyberspace, violence, like other phenomena originating in the physical world, manifests itself through forms, dimensions, and expressions specific to the virtual environment. Sexual violence, similarly, is one of the distressing realities of the physical world that also appears in cyberspace through altered forms and manifestations and has given rise to new criminal behaviors such as “sextortion,” “webcam sexual blackmail,” “cybersex trafficking,” “sex chat,” “online pornography,” “online pedophilic activity,” “hurtcore,” and similar practices.

Sextortion constitutes a non-physical form of coercion in cyberspace that is employed to extract sexual favors from a victim. In fact, the term refers both to a broad category of sexual exploitation in which abuse of power functions as the instrument of coercion and to sexual exploitation in which the threatened dissemination of sexual images or information operates as the coercive mechanism (De la Cerna, 2012). In addition, sextortion refers to a form of blackmail in which sexual information or images are used to extort money or sexual favors from the victim (Petz, 2022). It is therefore evident that social media and text messaging, as components of cyberspace, frequently constitute both sources of sexual material and instruments through which perpetrators threaten to share such material with others. One example of this type of extortion, itself constituting a form of sexual violence in cyberspace, occurs where individuals who have shared nude images of themselves online through messaging are subsequently compelled to pay money, perform sexual acts with the extortionist, pose before a camera, or engage in sexual acts (Petz, 2022). Through such conduct, hurtcore pornography may be produced. The term “hurtcore,” a combination of “hurt” and “hardcore,” refers to an extremely violent form of child pornography. Such material commonly involves degrading violence, physical injury, and even killing associated with the sexual abuse of children, and its content may be so violent that even many pedophiles reportedly find this genre of pornography repulsive.

Hurtcore has in fact been described as a fetish involving individuals who become sexually aroused by inflicting pain or even torture upon another person who is unwilling to participate. Thus, alongside the position of power exercised by the offender over the victim, one of the offender's sources of stimulation may be the victim's reactions to abuse and physical violence, such as crying or screaming in pain, which may further arouse the perpetrator (Evans, 2015).

Furthermore, sexual conduct involving webcam content, particularly among individuals who use webcams for flirtation and cybersex, constitutes another emerging manifestation of sexual violence in cyberspace (News, 2016a). Such conduct commonly involves a cyber offender pretending to be another person—for example, an attractive individual—and initiating sexual interaction with the victim. The cyber offender may simply display a prerecorded video of a performer from a cybersex webcam service with which the offender is sufficiently familiar and then, at points in the video where the performer appears to be typing on a keyboard, send messages to the victim so as to create the illusion that the performer appearing in the video is communicating directly with them (News, 2016b). The victim is then persuaded to remove clothing in front of a webcam and may also be induced to engage in sexual conduct such as masturbation. The cyber offender records the video and subsequently reveals the true purpose of the interaction by demanding money or other benefits, such as more explicit images of the victim, while threatening to publish the video publicly on video-sharing services such as YouTube or similar platforms or to send it to the victim's family members and friends if the offender's demands are not satisfied. Such behavior, known as webcam sextortion, constitutes another emerging form of cyber offending, and agencies dealing with these crimes have repeatedly reported increases in webcam blackmail, which affects victims across society, including young and older individuals and both men and women (News, 2016a). Webcam blackmail is also related to webcam trolling, which, similarly, constitutes a new manifestation of conduct involving sexual violence in cyberspace. Trolling is a form of online harassment that may assume the character of sexual harassment and sexual violence. Trolls may be regarded as the online counterparts of real-world bullies who exploit the powers and opportunities provided by cyberspace to intimidate, harass, and inflict violence upon others, including sexual violence. This process demonstrates that, alongside changes and transformations in cyberspace, sexual violence within this environment has also evolved and generated new forms of sexual misconduct.

3.2. From the Perspective of New Victims

It is evident that as offending becomes more widespread in cyberspace, the category of victims also expands, since every criminal act committed against others introduces additional victims into the population of those harmed. On this basis, new forms of victimization of women have also become widespread within the cyber paradigm, lending credibility to the proposition that victimization in cyberspace has become increasingly "feminized" (Hajizadeh Abadi, 2018). It has therefore been argued that, for offenders seeking to sexually exploit women, virtual spaces such as social networks, where online presence and repeated access to victims are possible, have replaced recreational venues and parks in the physical world (McKim, 2006). From the perspective of sexual violence in cyberspace, women are regarded as a particular category of victims because cyber victimization of men is generally focused on economic loss, whereas the "nature of women's victimization" is usually emotional and reputational, directly targeting their honor and social standing. Moreover, from a psychological perspective, women victims may have a lower tolerance for online humiliation than male victims, thereby exposing them to particularly serious risks and potentially irreparable forms of violence (Hajizadeh Abadi, 2018).

Alongside children and women, transgender persons constitute another category of victims who may be particularly vulnerable in cyberspace. Transgender individuals, by reason of their circumstances, may face greater exposure than others to crime and may therefore be at considerably higher risk of exploitation in the commission of crimes, particularly sexual offenses. Researchers in different countries have reported extensive sexual and financial exploitation of such persons through pornographic networks and websites, where, because of their particular circumstances, images and videos portraying them simultaneously in different sexual roles are commercially distributed on a large scale and heavily promoted (Ghani, 2022). In fact, transgender

persons constitute one category of victims of sexual violence in cyberspace who may in certain circumstances be exposed to sexual violence even more extensively than women. Because crises relating to gender identity can affect the individual's psychological and personal circumstances and may generate forms of social maladjustment in interaction with the society in which the individual lives, they may constitute a source of vulnerability, making the study of victimization through digital sexual harassment and violence especially important. Accordingly, transgender persons should be regarded as one of the emerging categories of cyber victims.

3.3. From the Perspective of New Perpetrators

In any event, the complexity, breadth, and even apparent boundlessness of cyberspace, resulting from its global character, have generated novel phenomena across different domains for which clear explanations using existing concepts and terminology are, if not impossible, at least extremely difficult. One such domain concerns crime and offending in cyberspace, where the diversity of criminal motives and objectives is as extensive as the diversity of users who commit crimes and offenses within it (Angelies, 2004). On this basis, developing a single classification of emerging cyber offenses and new cyber offenders is extremely difficult because of the interdisciplinary nature of the subject and the diversity of motives and purposes involved. Accordingly, some scholars, from a sociological perspective focusing on offenders' motives and the type of offense committed, classify perpetrators of sexual violence in cyberspace by connecting individual and social motivations with particular forms of offending, including the hypothesized relationship between revenge motives and offenses against honor and reputation and between motives involving the promotion of sexual permissiveness and offenses against public morality and chastity (Mahmoudzadeh, 2012). Such typologies differ from other classifications. Nevertheless, according to one of the more comprehensive classifications, cyber offenders may be divided into four categories: (1) the vindictive cyber offender; (2) the composed cyber offender; (3) the intimate cyber offender; and (4) the collective cyber offender. The vindictive cyber offender is a malicious person who threatens, harasses, and abuses victims more aggressively than offenders in the other three categories. The vindictive offender, who may also constitute a form of sexual offender, employs a variety of malicious tactics, such as malware, hacking, email flooding, and identity theft, to harass and inflict violence upon victims (Jahbin, 2018). The composed cyber offender, as the second category, differs from the vindictive offender in that the victim is targeted in a controlled, measured, and seemingly calm manner. The offender's primary objective is to create continuous tension and anxiety in the victim through threatening behavior. In addition to the composed offender, intimate cyber offenders constitute another category of cybercriminals who establish relationships with victims based on infatuation and psychological preoccupation in order to implement their criminal plans (Jaishankar, 2015). Sexual offenders, in particular, may regard this approach as a low-cost method of achieving their objectives in cyberspace. This category is itself highly diverse; some offenders may previously have had a personal relationship with the victim and may have been infatuated with that individual, thereby facilitating subsequent criminal conduct and violence, particularly sexual offending. Finally, the fourth category of emerging cyber offenders comprises collective cyber offenders, consisting of two or more individuals who jointly pursue a victim. Significantly, the computer skills of this group are often considerably higher than those of the three other categories (Jaishankar, 2015). Collective offending therefore represents a new form of cybercrime that illustrates the complexity of sexual violence in cyberspace. In any event, perpetrators of emerging forms of online sexual violence are not limited to these categories; nevertheless, these four types are among the most prevalent forms of emerging cyber offenders who continuously generate victims and novel forms of crime in cyberspace generally and in sexual violence-related cybercrime specifically.

4. Comparison of Iranian and English Criminal Policy (in the Narrow Sense) Regarding Sexual Violence in Cyberspace

Because sexual violence and harassment, whether occurring in the physical or virtual environment, constitute forms of social deviance and significant threats to cultural and social security and public order, different legal systems have adopted particular mechanisms, measures, and strategies to control,

confront, and eradicate them. Iranian and English criminal policies have likewise not remained indifferent to sexual deviance generally and sexual violence and harassment specifically. Both legal systems have developed their own frameworks, although the Iranian legal system is predominantly derived from Islamic jurisprudential principles. The present article examines these criminal policies primarily from a substantive perspective.

4.1. The Approach of the Iranian Legal System to the Criminalization of Violent Conduct in Cyberspace

Criminalization is the process through which the legislature, taking into account the fundamental norms and values of society and relying on accepted theoretical foundations, prohibits an act or omission and prescribes a criminal sanction for it (Aghababaei, 2005). Although the fundamental principle is human liberty and the avoidance of unnecessary restrictions on individual conduct and expression, the necessity of protecting the freedom of others requires the legislature, in accordance with societal values and norms, to establish restrictive legal rules as exceptions to the general principle of individual liberty. One such exception involves preventing sexual violence through legislation and criminalizing conduct that may be regarded as constituting sexual violence. Sexual violence in marital relationships is one of the most significant and recurrent forms of violence against women, yet it has not been expressly criminalized under Iranian criminal law. This undoubtedly leaves many victims without an effective legal remedy when they seek assistance from judicial authorities. It cannot reasonably be expected that all crimes and forms of social deviance can be controlled or diminished solely through criminal law and criminal sanctions; nevertheless, criminal law can respond to some extent to such abnormal social phenomena, since one of the functions of law is the moderation and regulation of violence (Joseph, 2006).

Accordingly, because laws in Iran are enacted within the framework of Islamic rules and principles, the legislature's approach to sexual violence remains substantially shaped by Islamic teachings and has shown resistance toward adopting certain human-rights-based components of criminalization concerning such forms of domestic violence. Thus, within Iran's criminal justice system, the legislature is, on the one hand, required under Article 4 of the Constitution to comply with Islamic principles when criminalizing conduct and determining punishments and, on the other hand, is expected to adhere to the general principles of modern criminal law and adapt components of criminal policy to contemporary social circumstances and international human rights obligations (Beigi, 2019). Criminalizing violent sexual conduct within marital relationships in order to prevent, deter, and reduce such violence under Iranian law could provide a necessary foundation for extending criminal protection to comparable forms of sexual violence occurring in cyberspace.

It is therefore necessary, before specifically addressing the criminalization of sexual violence in cyberspace, to consider the existing legal situation regarding criminalization of such conduct in the physical environment under Iranian law so that the subsequent analysis may proceed from a clearer foundation. As previously noted, violence occurring in marital relationships constitutes one form of violence in Iran that is not expressly addressed in the Islamic Penal Code. There is no explicit reference, for example, to marital rape and therefore no specific punishment has been prescribed for such conduct. The Civil Code, however, adopts a different approach by recognizing marital obedience as a duty of the wife. In its specific sense, obedience refers to the wife's performance of marital obligations. This means that whenever the husband desires sexual relations, the wife is expected to satisfy his sexual needs even when doing so is contrary to her own wishes. In such circumstances, psychological distress may lead to physical resistance, which can in turn cause or intensify physical, sexual, psychological, and verbal violence by the husband. The harm inflicted upon the woman in this form of violence may therefore be particularly serious. Indeed, experiencing violence involving rape, which falls within the broader category of gender-based offenses, may be especially distressing when committed by a husband. In such cases, the husband employs his individual, social, and psychological power and influence in order to have sexual intercourse with a wife who, for whatever reason, does not consent to the sexual relationship (Beigi, 2019). Accordingly, with respect to this form of sexual violence within marital relationships, the Iranian legislature has not merely failed expressly to criminalize the conduct but, by requiring women to submit to their husbands'

sexual demands under certain circumstances, may be regarded as legally validating certain forms of coercive sexual conduct.

Nevertheless, despite the silence of Iranian criminal law regarding sexual violence within marital relationships, the legal system has been somewhat more successful in addressing other forms of sexual violence outside the family and has enacted specific provisions applicable to sexually violent criminal conduct committed beyond the domestic sphere. These provisions may, in turn, provide a relatively strong criminal-law basis for formulating legislation necessary to criminalize forcible sexual misconduct and sexual violence in cyberspace. In this context, Article 619 of the Islamic Penal Code provides that anyone who, in public places or thoroughfares, harasses or molests children or women or insults them by words or gestures contrary to dignity and decency shall be subject to imprisonment and corporal punishment (Atashneh, 2012). This provision effectively criminalizes certain forms of sexually abusive verbal conduct in the physical environment and might be invoked in relation to sexual verbal and textual conduct directed against women and children in cyberspace. The importance of this provision lies, first, in the fact that harassment in streets and public places by men against women and children is treated as a criminally punishable form of misconduct. Because the term "harassment" is employed without restrictive qualification, conduct that according to social custom places another person under distress may fall within the scope of the provision. Second, insulting a woman or child in streets and public places is subject to a more serious punishment than ordinary insult (Atashneh, 2012). Accordingly, the provision may be interpreted as attributing a public dimension to verbal violence committed in public spaces and, by analogy, to such conduct in cyberspace through the transmission of audio files, images, videos, or texts containing insults generally and sexual insults specifically. From this perspective, the offense would be regarded as non-compoundable, meaning that the victim's withdrawal of the complaint would not necessarily exempt the offender from prosecution and punishment.

Furthermore, "persistent stalking," or, as some legal scholars describe it, "pursuit undertaken with the intention of harassment, intimidation, and causing fear in the person being followed," represents another form of violence that may acquire a sexual character depending upon the offender's motive. Because such conduct is often perpetrated by men against women, it may be categorized as a form of sexual violence, thereby raising the question of how Iranian law approaches the criminalization of such highly distressing and threatening conduct. In reality, providing a fixed definition of stalking is difficult because its conceptual boundaries have continually evolved and have sometimes been defined narrowly and sometimes broadly. Under a narrow definition, stalking is confined to following and surveillance behaviors and is commonly gendered in nature, with offenders generally being men and victims generally being women (Gholamloo, 2020). Under a broader definition, stalking includes, in addition to following and surveillance, other forms of harassing conduct such as sexual harassment and physical injury, although such an approach considerably expands the concept (Choon & Sheridan, 2017).

Based on this definition and from the perspective of the manner in which stalking is committed, most traditional stalking and surveillance occurs in the physical environment. Endless letter writing, repeated telephone contact, leaving messages on vehicle windows or at the victim's home or workplace, repeated and continuous following, threats, declarations of affection, and sending gifts despite the wishes of the person being pursued are among the principal manifestations of stalking in the physical world (Hirtenlehner et al., 2012). However, in view of the subject of the present study and the discussion of violence in cyberspace, it is evident that manifestations of this form of violence have become broader online and, because of the offender's anonymity arising from the nature of cyberspace, have acquired more complex forms capable of reproducing violence in new ways. Through the Internet, offenders can obtain information concerning victims with few practical limitations and use that information to harass and intimidate them. Stalking in cyberspace may therefore assume particularly dangerous forms because offenders may easily intrude upon individuals' privacy and harass them (Gholamloo, 2020) without fearing disclosure of their identity and consequent legal prosecution. Examples include sending harassing messages through online communication platforms such as email, Telegram, WhatsApp, and Instagram or sending spam to the victim, potentially resulting in the receipt of

thousands of unsolicited messages each day (Wall, 2001). Accordingly, where the recipient does not consent, repeated and persistent messaging, regardless of the content and even where the content appears ordinary, may constitute stalking. When motivated by sexual objectives, such conduct may become one of the most distressing forms of sexual violence requiring a specific legislative response.

Nevertheless, current Iranian criminal legislation does not recognize a separate offense expressly entitled persistent stalking, and such conduct can only be addressed indirectly by reference to existing related provisions, including Articles 619, 638, and 641 of the Ta'zirat Book of the Islamic Penal Code. Article 638 may potentially be invoked in relation to verbal sexual assaults and even unwanted physical touching because, notwithstanding ambiguous expressions such as "public chastity," which is not specifically defined in the Penal Code, and the broad phrase "prohibited act," each of which requires interpretation and has generated divergent interpretations, certain stalking behaviors may fall within the second part of this provision (Salehi, 2018). For instance, behaviors such as staring or making sexually suggestive looks at an unrelated woman may constitute harassment and are also regarded as religiously prohibited conduct; under particular circumstances, including repetition and persistence, such acts may substantively constitute stalking (Salehi, 2018). Such conduct clearly represents a form of sexual violence in the physical environment and may likewise have an online equivalent where women and children are subjected to persistent harassment through various messaging platforms.

Likewise, as noted previously, Article 619 of the same law may be interpreted as a provision under which stalking or surveillance of others, whether in the physical environment or cyberspace, may be treated as criminal conduct (Atashneh, 2012). Just as the traditional form of persistent stalking involves following an individual in streets or other physical locations, repeated telephone contact, transmission of audio files, texts, or images through messaging applications, online monitoring, and digital surveillance may similarly constitute forms of harassment and intrusion that fall within the rationale of such legal provisions.

Moreover, with the development of technology, the Iranian legislature has criminalized one form of conduct that may constitute persistent harassment, namely telephone harassment, which may arguably be extended to other forms of harassment conducted predominantly with sexual motivations in cyberspace and thereby amounting to sexual violence. Article 641 of the Ta'zirat provisions criminalizes creating harassment through telephone or other telecommunications devices. Although the provision expressly refers to telephone communications, it is capable of broader interpretation in relation to harassment conducted through cyberspace because the concept of harassment is formulated in general terms and can encompass different forms of disturbing conduct. Online harassment, particularly where it carries sexual characteristics and may therefore be classified as violence, could accordingly fall within the scope of such a provision. Nevertheless, the existence of Article 641 should not be interpreted as eliminating the need for new legislation specifically criminalizing identifiable online harassment, particularly sexual verbal and written harassment. The prevalence and broad scope of cyberspace require the legislature to develop new laws and criminalize conduct that can be categorized as sexual violence. It may therefore be concluded that the Iranian criminal justice system has not precisely and specifically criminalized sexual violence generally, and sexual violence in cyberspace particularly, under clearly designated legal provisions; rather, such criminalization can only be inferred indirectly from various statutory provisions. Iranian criminal law does criminalize certain acts involving illicit sexual relationships conducted through cyberspace, but illicit relationships and sexual violence constitute two distinct legal categories and should not be treated as equivalent.

4.2. The Approach of the English Legal System to the Criminalization of Violent Conduct in Cyberspace

The prevalence of sexual violence in England has resulted in this phenomenon being addressed seriously within the country's criminal policy and being subjected to criminalization. Reports issued by the Ministry of Justice, the Office for National Statistics, and the Home Office in a joint bulletin concerning sexual violence in England and Wales have indicated that approximately 85,000 women are raped each year on average and that more than 400,000 women experience sexual violence annually (Kessel & Bernstein, 2003). These figures

demonstrate that sexual violence constitutes a significant crime-related problem in England and is increasingly influenced by developments in cyberspace, since comparative experience demonstrates that cyberspace has affected sexual violence in both quantitative and qualitative respects. This situation has led to the criminalization of sexual violence in specific contexts, including forcible sexual offenses, sexual offenses against children, coerced sexual relations within marriage, and related conduct.

Although legislation in England, as a common-law legal system, is historically grounded in custom and judicial precedent, the legislature has recognized that reliance upon case law alone is insufficient in relation to sexual offenses. Since 1956, specific statutes dealing with sexual offenses have therefore been enacted and amended in areas including offenses against children and forcible sexual offenses, ultimately culminating in the Sexual Offences Act 2003, which criminalized a broad range of sexual acts under categories including rape and sexual assault (Niknejad, 2024). One form of sexual violence, of which women are predominantly victims and which has been criminalized under English criminal law, is rape within marital relationships. This form of sexual violence, involving coercing a victim into sexual activity within marriage beyond the limits of consent, was not historically recognized as a crime under English law because the legal position was based on the belief that a husband could not be convicted of raping his wife. This doctrine, originating in the eighteenth century, rested upon the assumption that by entering marriage a woman had given continuing consent to sexual intercourse with her husband under all circumstances. When rape was formally defined in statutory law, the offense was initially understood in practice as capable of occurring only outside marriage, subject to limited exceptions where a judicial order or equivalent circumstance clearly demonstrated the withdrawal of the wife's consent (Motamedi Mehr, 2001). In other words, the legal conception of rape came to involve unlawful sexual intercourse with a woman who had not consented, where the man knew of the absence of consent or was reckless as to it. In any event, criminalizing sexual violence within marriage in England involved considerable debate between opponents and supporters until the Court of Appeal ultimately rejected as unrealistic the premise that marriage constituted permanent consent to sexual intercourse and recognized that no legal rule prevented a husband from being convicted of raping his wife. This position was subsequently affirmed, and legislative reforms ultimately incorporated marital rape within the modern law of sexual offenses (Mirmohammad Sadeghi, 2009). Accordingly, English law criminalizes forcible intercourse with a spouse and lesser forms of sexual assault, including unwanted kissing and touching, where these acts are committed without consent (Niknejad, 2024). English criminal law has also historically regulated certain forms of anal intercourse as sexual offenses, although the scope and legal treatment of such conduct have changed significantly over time.

English law likewise recognizes and criminalizes conduct that may be described as "sexual assault," or coerced sexual touching. Under this framework, any intentional sexual touching of another person, where the perpetrator knows or is reckless as to the victim's lack of consent, may constitute an offense. Sections 3 and 7 of the Sexual Offences Act 2003 address relevant conduct directly, while other provisions criminalize related acts that may indirectly involve non-consensual sexual touching (Niknejad, 2024). In any event, within English law, consent plays a fundamental and determinative role in sexual offenses, and, subject to limited exceptions, the absence of the victim's consent constitutes the principal condition for establishing such offenses. Given the degree of attention paid by English law to sexual violence against women in the physical environment, it is evident that the legal system cannot remain indifferent to comparable offending in cyberspace. Accordingly, legislation and criminal policy have increasingly provided protection for victims of online abuse by criminalizing coercive and abusive conduct. Such legal measures particularly target individuals who psychologically and emotionally abuse spouses or intimate partners through online methods. Controlling or coercive behavior employed to harm, punish, intimidate, or subordinate victims may encompass a wide range of online conduct, including preventing the victim from engaging in online social interaction, restricting digital access to family members and friends or financial resources, monitoring the victim through technologies such as mobile tracking applications, and threatening to obtain or disseminate personal information (Niknejad, 2024). Such conduct may be

intended to render the victim submissive or dependent or to facilitate sexual extortion.

In addition to women, children, as previously noted, constitute victims of violence generally and sexual violence specifically in both offline and online environments, and English law treats sexual violence against children as a criminal matter.

Technological developments in cyberspace, despite their positive economic and social achievements, have also created significant opportunities for abuse involving violations of human dignity and rights, social norms, and ethical values. Certain groups, particularly children and adolescents, are more vulnerable than others to infringements of fundamental rights and to physical and psychological harm. Disturbing phenomena such as child modeling, child pornography, and child sex tourism have been facilitated through modern information and communications technologies. Consequently, over recent decades, protecting children in cyberspace and combating and preventing various forms of exploitation and abuse of children and adolescents have become major concerns for governments and international organizations. England is among the countries that have criminalized the distribution, sharing, and production of indecent images of children as forms of sexual violence against minors (Hosseini Akbarnejad, 2020). In particular, the Protection of Children Act 1978 made England one of the early jurisdictions to recognize the need to prevent dissemination of such material, and later legislative reforms and sentencing developments continued to reinforce the importance of this area.

In this respect, communication with children and adolescents in cyberspace for the purpose of sexual harassment or unlawful sexual interaction may constitute an offense under laws governing sexual communications and indecent images. Such conduct may include sending images or videos of oneself or others, semi-nude images or videos, or sexual messages (Hosseini Akbarnejad, 2020). The relevant child-protection legislation expressly criminalizes certain forms of production, publication, and distribution of indecent content involving children and provides criminal sanctions for offenders (Hosseini Akbarnejad, 2020). In cases prosecuted on indictment, sentencing is determined according to the seriousness and category of the offense. Relevant categories include possession of indecent images of children, distribution or sharing of such images, and production of indecent images (Hosseini Akbarnejad, 2020). Another manifestation of sexual violence against children is online sexual exploitation and child sex tourism; English law also permits the prosecution of British nationals for certain sexual offenses committed against children abroad.

4.3. The Approach of the Iranian Legal System to Punishment and Responses to Violent Conduct in Cyberspace

Sentencing constitutes one of the most important stages of the criminal process and concerns the determination of punishment at the judicial stage (Gharghi, 2021). In addition to the substantive element of criminalization discussed in the preceding section, the element of punishment plays a highly significant role in regulating criminal relationships and conduct in both physical and virtual environments. The principal provisions relevant to punishment for cybercrimes, including conduct involving sexual violence, are contained in Iran's Computer Crimes Act of 2009. The 2020 Law on the Protection of Children and Adolescents constitutes another statute within the Iranian criminal justice system that may be applied to punish perpetrators of sexual violence against children. Chapter Four, Part One of the Computer Crimes Act, under the heading "Crimes against Public Chastity and Morality," contains provisions from which the punishment of certain forms of sexual violence can be inferred. Article 14 provides criminal sanctions for anyone who, through computer or telecommunications systems or data carriers, publishes, distributes, trades, produces, stores, or retains obscene content for commercial purposes or corruption. Because sending obscene images and textual content to individuals, particularly women and children, may constitute a form of sexual harassment and violence in cyberspace, the provision can potentially be invoked against offenders who inflict sexual violence in this manner (Razavi Fard, 2016). As previously explained, sexual violence in cyberspace may predominantly take the form of verbal, written, textual, or comparable conduct containing sexual material communicated to individuals against their wishes or consent, as well as dissemination of private images or videos.

On this basis, the supplementary provisions associated with Article 14 of the Computer Crimes Act prescribe sanctions for conduct involving indecent or obscene

content and establish punishment for different forms of dissemination (Razavi Fard, 2016). Subsequent provisions provide penalties for acts in cyberspace that may, depending upon the circumstances, constitute forms of sexual violence. In particular, the legislation criminalizes the transmission of obscene content and defines such content as images, audio, or real or simulated textual or visual material depicting complete nudity, genital organs, sexual intercourse, or sexual acts (Razavi Fard, 2016). Such provisions explicitly recognize the sexual character of the prohibited conduct and may provide a legal basis for punishing individuals who distribute sexual images for purposes such as revenge, sexual extortion, or organized commercial exploitation, thereby producing harms that may reasonably be classified as sexual violence.

Article 15 of the amended Computer Crimes Act arguably places even greater emphasis than Article 14 on cyber offenses related to sexual violence. The provision criminalizes conduct through computer or telecommunications systems or data carriers involving incitement, encouragement, threats, enticement, deception, facilitation, or instruction relating to access to obscene content and also prohibits inciting, encouraging, threatening, inviting, or deceiving individuals into committing offenses against chastity, using narcotic or psychotropic substances, committing suicide, engaging in sexual deviance, or carrying out violent acts (Razavi Fard, 2016). Both parts of the provision therefore prescribe punishment for conduct that can clearly constitute manifestations of sexual violence. Incitement, encouragement, threats, or invitations relating to sexual misconduct may, depending upon circumstances, constitute forms of sexually violent behavior. Likewise, facilitating access to sexually explicit images through deception, inducement, threats, or coercion, particularly where the purpose is to exploit and harass the victim, may fall within the conceptual framework of sexual violence. Articles 14 and 15 of the Computer Crimes Act may therefore be regarded as implicitly and, in certain respects, expressly determining sanctions for online sexual exploitation and sexual violence.

Furthermore, because children and adolescents constitute significant victims of sexual violence both in cyberspace and the physical environment, another aspect of the Iranian sentencing framework may be interpreted through reference to the Law on the Protection of Children and Adolescents. Chapter Three of this law, entitled “Crimes and Punishments,” includes provisions addressing sexual abuse resulting from serious and persistent negligence and prescribes criminal sanctions for such conduct (Hosseini Akbarnejad, 2020). Accordingly, the law establishes punishment for certain forms of sexual abuse and violence affecting children and adolescents.

Moreover, the law addresses sexual violence and sexual abuse more explicitly by criminalizing a broad range of conduct against children and adolescents. Such conduct includes contact sexual abuse committed by relatives or through force, other forms of contact sexual abuse, non-contact sexual abuse involving relatives or coercion, other forms of non-contact sexual abuse, sexual exploitation of children through pornography or sexual abuse, providing obscene or indecent content to children, using children to prepare, produce, distribute, reproduce, display, sell, or retain obscene or indecent audiovisual materials, importing, exporting, reproducing, publishing, offering, trading, uploading, possessing, or retaining obscene or indecent content involving children, and establishing online communication with a child or adolescent for the purpose of sexual harassment or unlawful sexual relations (Hosseini Akbarnejad, 2020). The law further prohibits transactions involving children, with aggravated penalties where such conduct is undertaken for prostitution, pornography, economic exploitation, organ removal, or involvement of the child in criminal activities. These provisions demonstrate that children are particularly susceptible to sexual exploitation and the violence associated with it and that Iranian legislation has attempted to identify many of the methods through which offenders may sexually abuse children. Consequently, both the Computer Crimes Act and the Law on the Protection of Children and Adolescents contain provisions establishing punishment for conduct related to sexual violence, which predominantly affects women and children but is not limited to those groups. Nevertheless, legislative gaps remain, particularly because of the fluid and rapidly changing character of cybercrime, and the legislature must therefore adopt more serious measures in both criminalization and sentencing.

4.4. The Approach of the English Legal System to Punishment and Responses to Violent Conduct in Cyberspace

Given the criminalization of sexual violence in both offline and online environments, English law has not remained silent regarding punishment for such conduct and has expressly established sanctions in this field. As previously indicated, sexual violence, including rape, has been addressed through successive sexual-offense legislation and broader criminal justice reforms. The Sexual Offences Act 2003 introduced fundamental changes to this area. Under the Act, rape is punishable by life imprisonment, while English criminal justice policy also provides a range of community-based and supervisory measures depending upon the offense and circumstances (Niknejad, 2024). Under the modern approach, the mental element of sexual offenses includes intention and, depending upon the statutory offense, concepts relating to awareness, recklessness, and the reasonableness of belief in consent.

Accordingly, English criminal law recognizes rape where sexual penetration occurs without the voluntary agreement of a person who possesses the freedom and capacity to make that choice. Violence, unconsciousness, and deception are among circumstances from which the absence of consent may be presumed (Akrami, 2016). This is significant because, historically, rape law placed greater emphasis upon the use of force by the offender, whereas contemporary English law does not require force as an essential condition (Elliott, 2014). The central aggravating substantive element is the absence of the victim's consent, which the prosecution must establish in order to obtain a conviction (Jefferson, 2013). Thus, in English law, absence of consent is sufficient for the constitution of relevant sexual offenses, and it is not always necessary to demonstrate the use of force or threats by the offender (Wilson, 2011), nor must the woman necessarily show active physical resistance or expressly communicate dissatisfaction (Jefferson, 2013). English law provides statutory evidential and conclusive presumptions through which the absence of consent may be established (Wilson, 2011). The statutory presumptions are divided into two categories: evidential presumptions, which may be rebutted by contrary evidence, and conclusive presumptions, which are not rebuttable.

Under Section 75 of the Sexual Offences Act 2003, where the defendant has engaged in the relevant act and certain specified circumstances exist of which the defendant was aware, the law presumes, in the absence of sufficient evidence to the contrary, that the complainant did not consent and that the defendant did not reasonably believe that the complainant consented. Such circumstances include the use of violence immediately before or during the relevant act; causing the complainant to fear immediate violence against themselves or another person; unlawful detention of the complainant while the defendant is not detained; the complainant being asleep or otherwise unconscious; a physical disability preventing the complainant from communicating consent; and the administration or causing the complainant to take a substance without consent where that substance renders the complainant stupefied or overpowered (Akrami, 2016).

Section 76 of the Sexual Offences Act 2003 establishes conclusive presumptions concerning consent. Where it is proved that the defendant intentionally deceived the complainant as to the nature or purpose of the relevant act or induced consent by impersonating a person known personally to the complainant, the law conclusively presumes that the complainant did not consent and that the defendant did not believe in consent (Jefferson, 2013). Where such deception or inducement is absent, or where it is not intentional, these conclusive presumptions do not apply. Historical cases concerning deception and consent illustrate the limits of the doctrine, including cases in which false representations regarding payment were regarded as insufficient to invalidate consent because the deception did not concern the nature of the act or the identity of the person involved (Allen, 2007).

It is therefore evident that the sensitivity of English sexual-offense law to the absence of consent in the offline environment has important implications for online conduct, and comparable principles have increasingly been applied or extended to cyberspace. On this legal foundation, English criminal policy has increasingly treated forms of online sexual harassment, including the non-consensual transmission of sexual images, as criminal conduct, and offenders may face imprisonment depending upon the nature and seriousness of the offense. The sending of unsolicited sexual images through social networks, dating applications, and other

messaging services may therefore constitute a criminal offense. The development of such legislation reflects the widespread incidence of sexual harassment in cyberspace. Research conducted in 2020, for example, indicated that a substantial proportion of girls between the ages of 12 and 18 had received unsolicited nude images from boys or men, while earlier survey research similarly suggested that many young women had experienced comparable conduct. These developments contributed to broader legislation addressing online safety and imposing greater legal responsibility upon social-media platforms, search engines, and other websites to respond to unlawful and harmful content and communications. English criminal policy has therefore increasingly emphasized the protection of women and girls, longer custodial sentences for violent and sexual offenders, improved reporting opportunities for victims of domestic abuse, and expansion of victim-support services (Niknejad, 2024). Criminalization of these online acts therefore communicates a clear message that perpetrators may be subjected to imprisonment proportionate to the nature and extent of their conduct.

In addition to punishment for online sexual harassment offenses, of which women are among the principal victims, children and adolescents constitute another major category of victims of sexual violence in cyberspace and are specifically protected under English criminal policy. Sentencing reforms relating to offenses involving indecent images of children have introduced increasingly serious penalties and structured sentencing categories. In general, punishment is differentiated according to both the nature of the conduct and the seriousness of the images involved.

First, possession of indecent images of children—including photographs, films, graphic depictions, drawings, and other visual material—is categorized according to severity. At the highest level, material explicitly depicting penetrative sexual activity, sexual activity involving animals, or sexual sadism attracts the most serious punishment. Lower categories include images depicting sexual activity with children without penetration and other indecent images falling outside the first two categories. Depending on seriousness, such offenses may result in custodial sentences ranging from relatively short periods to several years (Hosseini Akbarnejad, 2020).

Second, distributing or sharing indecent images while possessing them attracts more serious punishment than simple possession, with penalties increasing according to the seriousness of the material disseminated. Distribution of the most serious category may attract multi-year custodial sentences, while distribution of lower-category material remains punishable by imprisonment.

Third, producing or creating indecent images of children attracts particularly serious penalties. Production of images falling within the highest category may result in lengthy imprisonment, while production of lower-category material also carries substantial custodial sentences (Hosseini Akbarnejad, 2020). Thus, English law has developed a comparatively comprehensive approach to identifying cyber offenses related to sexual violence and has prescribed differentiated punishments according to the type and seriousness of the offending conduct.

5. Requirements and an Appropriate Model for Aligning Iranian Criminal Policy (in the Narrow Sense) with Responses to Sexual Violence in Cyberspace

Given the expansion of cybercrime, the need to develop appropriate legal measures within criminal policy is felt particularly strongly at the substantive level. The following discussion therefore examines the principal requirements for such development.

5.1. From the Perspective of Criminalization

The legitimacy of criminalization requires adherence to principles such as necessity, respect for privacy and human rights standards, proportionality between crime and punishment, legality, and other fundamental criminal-law principles.

Accordingly, with respect to violence in cyberspace generally and sexual violence in cyberspace specifically, three broad approaches to criminalization can be identified in different jurisdictions.

(a) Some countries, including France, Australia, the Philippines, and Spain, have independently criminalized cyber violence because of the serious harms associated with it, including suicides resulting from online abuse. In France, cyber violence, of which sexual violence may constitute one dimension, has been addressed through offenses concerning cyberbullying and harassment,

while Spanish criminal legislation likewise provides sanctions for repeated and persistent electronic harassment. Examination of these legal approaches demonstrates that online harassment, including sexual violence committed through cyberspace, has been subjected to specific criminalization. The Philippines likewise enacted anti-cyberbullying legislation in 2013 and expressly addressed the criminalization of online harassment (Hosseini, 2023).

(b) In some countries, including England and Germany, cyber violence has not historically been criminalized as a single independent and specific offense (Hosseini, 2023); rather, relevant conduct has been addressed within other statutory offenses expressly or by implication.

(c) In the United States, because legislation exists at both federal and state levels, a combination of the two preceding approaches may be observed. Comparing Iran's approach with these models reveals that, although Iran has enacted the Computer Crimes Act and other legislation relating to cyberspace, sexual violence and sexual harassment in cyberspace, including related forms of cyberbullying, have not been expressly criminalized as distinct offenses. For the reasons discussed below, there is therefore a clear need to align Iranian criminal policy more closely with legal systems that regulate such conduct systematically and in accordance with established principles of criminalization.

(1) Dangerous and harmful consequences of cyber sexual violence: Cyber violence in general has been described as a form of "social online terror" that may be pervasive, potentially devastating, and associated with self-harm and suicide among young people. Surveys conducted internationally have indicated that substantial proportions of adolescents have experienced online abuse. Reliable statistical data of comparable scope are not readily available in Iran for various reasons. Accordingly, one justification for aligning Iranian criminal policy with approaches that criminalize sexual violence in cyberspace is the need to protect the physical and psychological integrity of adolescent and young victims and provide effective criminal-law protection.

(2) The distinction between cyberspace and the physical environment and the need for differentiated criminalization: Because of the distinctive characteristics of cybercrime, new forms of offending and social harm, including sexual violence and harassment, manifest themselves differently online than in traditional environments. Cyberspace has transformed conventional criminal law to such an extent that definitions of offenses in digital environments do not always correspond to classical definitions. Consequently, cybercrime cannot be effectively regulated solely through criminal policies designed for the physical world. The speed, scale, ease, low cost, transnational character, and anonymity of cyber offending have generated a distinct category of criminality requiring specialized penal responses. Because of the particular problems arising from the virtually unlimited nature of cyberspace and the limitations of classical criminal-law doctrine, alternative concepts of criminal responsibility, including forms of vicarious criminal liability within differentiated criminal policy, have also been proposed (Kazemi Sanjabi, 2017). Criminalization of such conduct therefore appears necessary within Iranian criminal policy.

(3) Inadequacy of existing criminal legislation: Because sexual violence and its conceptual boundaries are not clearly defined in Iranian criminal law and criminal policy, even assuming that related existing criminal provisions are applicable, effective implementation remains problematic. Applying existing criminal classifications first requires an adequate statutory definition of the phenomenon itself. Several deficiencies of Iran's 2009 Computer Crimes Act may be identified in relation to online sexual violence. Certain provisions concerning publication of another person's audio or image focus upon alteration, distortion, or awareness of such manipulation. Yet offenders may disseminate another person's image or audio without alteration or distortion. Moreover, the legislation does not specifically address violent conduct or its sexual dimensions in connection with such dissemination. In sexual violence, offenders may use the dissemination of another person's private information as a means of sexual extortion, a form of abuse insufficiently addressed by the Computer Crimes Act. Similar concerns arise under other provisions of the statute. Furthermore, cyber sexual violence may cause serious non-pecuniary harm to victims, while the Computer Crimes Act does not adequately address such injury (Hosseini, 2023). In view of these deficiencies, Iranian criminal policy should expressly criminalize sexual exploitation and violence committed by cyber offenders or otherwise move toward

the approaches adopted by jurisdictions with more developed criminal policies in this area.

(4) The harm principle: Another principle capable of justifying criminalization is the harm principle, according to which conduct should be subject to criminal punishment where it causes harm to others (Roustaei, 2015). Because sexual violence in cyberspace can harm victims' reputation, dignity, bodily integrity, and psychological well-being, the harm principle provides a strong justification for requiring Iranian criminal policy to take urgent steps toward its criminalization. Accordingly, Iranian criminal policy should establish sexual violence in cyberspace as an independent criminal category while simultaneously respecting the presumption of innocence and other principles that confer legitimacy upon criminalization.

5.2. From the Perspective of Punishment

In the absence of explicit criminalization of sexual violence in cyberspace, the Iranian legislature necessarily remains limited in developing an effective sentencing framework for such conduct. In other words, Iranian criminal policy also requires the formulation of specific sentencing provisions in this field. Although Chapter Six of the Computer Crimes Act addresses certain aspects of punishment in cyberspace, one of the most significant developments introduced by the legislation was the recognition of criminal liability for legal persons under provisions governing corporate criminal responsibility.

As repeatedly discussed throughout this study, the use of modern communication technologies, particularly the Internet and cyberspace, has created new opportunities for offenders to commit crimes. Where criminal law within a society fails to evolve in accordance with technological developments, significant forms of offending may remain inadequately punished. Among the principal instruments available to criminal justice systems for combating emerging crimes are criminalization, development of new sentencing approaches, innovative dispute-resolution mechanisms, and new forms of sanctions (Razavi Fard, 2016). Iranian criminal policy has not yet sufficiently developed these mechanisms in the field of punishment for cyber sexual violence and therefore needs to formulate sentencing techniques adapted specifically to cyberspace and to sexual violence committed within it. Furthermore, although the Computer Crimes Act marked an important development by recognizing criminal liability of legal persons, and although many cyber offenses may involve corporations or organizational actors, criminal liability of legal persons alone does not resolve the sentencing problem associated with sexual violence in cyberspace. Supplementary sanctions may also contribute to a differentiated penal policy for cyber offenders. For example, courts in other jurisdictions have in some cases prohibited individuals convicted of online sexual offenses from using social networks (Danesh Nari, 2018). Such comparative experiences may provide Iranian legislators with useful models for developing innovative punishments for new forms of cybercrime, including sexual violence.

6. Conclusion

Victimization through sexual offenses—including sexual violence in the home, sexual harassment in society, sexual abuse in the workplace, and, as examined in the present study, sexual violence in cyberspace—is a distressing experience capable of producing severe consequences for different members of society, particularly women, children, and transgender persons. A substantial proportion of victims may experience consequences such as depression, fear, substance dependence, and persistent anxiety following incidents of sexual violence, while in more severe cases some victims may engage in self-harm or suicide. In view of these consequences and the extensive reach of sexual violence in cyberspace resulting from the distinctive characteristics of the digital environment, many governments have sought to revise and update their criminal policies at the legislative, judicial, and executive levels or to develop independent criminal policies concerning cybercrime, including online sexual violence. On this basis, the present study reaches several conclusions. First, although England has independent legislation addressing sexual violence generally, its criminal policy regarding sexual violence in cyberspace still contains certain gaps and inconsistencies. Iranian criminal policy, although it criminalizes and punishes cybercrime generally, lacks an independent and comprehensive legal framework specifically addressing sexual violence, particularly in cyberspace. Second, compared with Iranian criminal policy, English law has identified and addressed cyber offenses involving sexual

violence in a comparatively more comprehensive manner and has established differentiated sanctions appropriate to different forms and levels of offending. Third, whereas Iranian law addresses certain forms of sexual violence against women and children primarily through provisions designed for the physical environment, English criminal policy has increasingly treated violence generally and sexual violence specifically against children and women as relevant to both offline and online environments. Fourth, in England, consent performs a fundamental and determinative function in sexual offenses, and, subject to limited exceptions, the absence of the victim's consent constitutes the principal criterion for criminal liability. The seriousness with which English law treats sexual violence against women in the physical environment therefore extends naturally to criminalization of analogous conduct against them in cyberspace. Fifth, examination of Iranian criminal policy concerning sexual violence demonstrates that existing cybercrime legislation does not provide a sufficiently coherent framework for sentencing natural persons who constitute the principal perpetrators of many cyber offenses, nor does the sentencing system adequately address violence generally or sexual violence specifically in cyberspace. Iranian criminal policy should therefore develop both effective sanctions applicable to natural persons and a specific sentencing framework for sexual violence committed in cyberspace. Ultimately, comparison of the criminal policies of the two countries supports the recommendation that Iran move toward a coherent and independent criminal policy for criminalizing and punishing violence in cyberspace and establish an appropriate and specialized criminal procedural framework for such offenses. Such reform constitutes both a social and a legal necessity.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Aghababaei, H. (2005). Jurisprudential Discourse and Criminalization in Crimes against the Security of the Nation and the State. *Fiqh and Law*(5).

Akrami, R. (2016). The Element of Coercion in Zina from the Perspective of Islamic Jurisprudence and Iranian and English Criminal Law. *Comparative Research on Islamic and Western Law*, *3*(1).

Allen, M. (2007). *Criminal Law*. Oxford University Press.

Angelies, G. (2004). *Cybercrimes*. Supreme Council for Judicial Development; Secretariat of the Supreme Council of Information.

Atashneh, M. (2012). Examining the Causes, Factors, and Effects of Sexual Crimes against Women from the Perspective of Iranian Criminal Law. *Woman and Culture*, *3*(11).

Beigi, J. (2019). Criminalization of Sexual Violence in Marital Relationships with Emphasis on International Human Rights Instruments. *International Studies*, *16*(2).

Choon, H., & Sheridan, L. (2017). Is this stalking? Perceptions of stalking behavior among young male and female adults in Hong Kong and mainland China. *Journal of interpersonal violence*.

Danesh Nari, H. R. (2018). *Social Networks as a Tool for Committing Crime*. Mizan Publishing.

De la Cerna, M. (2012). Sextortion.

Elliott, C. (2014). *Criminal Law*. Pearson Education Limited.

Evans, R. (2015). 5 Things I Learned Infiltrating Deep Web Child Molesters.

Fattahian, M. (2017). An Examination of the Global Causes of Increasing Cyber Violence against Women. *Ghanoonyar*, *3*.

Ghani, M. (2022). An Examination of Adult Victimization by Digital Sexual Harassment with Attention to Transgender Individuals. *Criminal Law Research*, *13*(1).

Gharghi, J. (2021). Criteria for Distinguishing Substantive from Procedural Laws in Terms of Objectives, Characteristics, and

Functions in Iranian Criminal Law. *Comparative Criminal Jurisprudence*, *1*(4).
Gholamloo, J. (2020). A Comparative Study in Iranian and United States Criminal Law. *Criminal law and Criminology Studies*, *50*(2).
Hajizadeh Abadi, M. A. (2018). Etiology of Women's Victimization on Social Networks: A Case Study of Facebook. *Woman and Society*, *9*(3).
Hematpour, B. (2017). Identifying and Sociologically Explaining Violence against Women in Cyberspace: A Case Study of Women Aged 20–45 in Tehran. *Women's Research*, *8*(4).
Hirtenlehner, H., Starzer, B., & Weber, C. (2012). A differential phenomenology of stalking. *International Review of Victimology*, *18*.
Hosseini Akbarnejad, H. (2020). Criminal Protection of Children against Online Abuse in Iranian and English Law and International Instruments. *Legal Research*(44).
Hosseini, S. A. (2023). Assessing the Need to Criminalize Cyberbullying in Iranian and American Criminal Law. *Comparative Law*, *10*(1).
Jahbin, Z. (2018). Factors Affecting the Commission of Crime in Cyberspace from the Perspective of Judges of the Tehran Computer Crimes Prosecutor's Office. *Intelligence and Criminal Research*, *13*(3).
Jaishankar, K. (2015). *Cyber Criminology*. Amin Police University Press.
Jefferson, M. (2013). *Criminal Law*. Pearson Education Limited.
Joseph, Y. E. D. (2006). The One who is More Violent Prevails: Law and Violence from a Talmudic Legal Perspective. *Canadian Journal of Law and Jurisprudence*, *19*(2).
Kazemi Sanjabi, B. (2017). *Computer and Cyber Crimes*. Ghanoonyar Publications.
Kessel, E., & Bernstein, D. A. (2003). *Criminal Behavior*. NAJA Research Center.
Mahmoudzadeh, S. (2012). *A Sociological Study of Individuals' Motives and the Types of Crimes Committed on the Facebook Social Network* Alzahra University, Faculty of Economics and Accounting].
McKim, J. (2006). Pimp pleads Guilty to Prostituting minor. http://www.ocregister.com/ocregister/news/atoz/article_1209170.phd
Mirmohammad Sadeghi, H. (2009). A Comparative Study of the Concept of Coercion in Sexual Crimes. *Dadresi*(76).
Motamedi Mehr, M. (2001). *Protection of Women against Violent Crimes: England's Criminal Policy*. Barg-e Zeytoon.
News, B. B. C. (2016a). The Skype sex scam - a fortune built on shame.
News, B. B. C. (2016b). Webcam blackmail cases have doubled, police say.
Niknejad, A. (2024). Sexual Violence against Women in Iranian and English Criminal Law. *Teachings of Jurisprudence and Criminal Law*, *3*(2).
Petz, S. (2022). Teen boys make up majority of victims of recently reported sextortion crimes, new data shows.
Razavi Fard, B. (2016). Criminal Liability in Cyberspace under Iranian Law. *Criminal Law Research*, *5*(16).
Roustaei, M. (2015). A Comparative Study of the Harm Principle and the No-Harm Rule in Justifying Criminal Intervention. *Comparative Law Research*, *19*(2).
Salehi, S. H. (2018). A Jurisprudential and Legal Examination of Surveillance and Its Exceptions. *Jurisprudential Foundations of Islamic Law*(21).
Shadmani, M. (2015). Examining the Challenges Facing Women in Cyberspace. *Studies on the Protection of Women's Rights*(2).
Wall, D. (2001). *Crime and the Internet*. Routledge.
Wilson, W. (2011). *Criminal Law: Doctrine and Theory*. Pearson Education Limited.